Amendments to the Drawings:

The attached sheets of drawings includes changes to Figs. 2-3. These sheets, which include Figs. 2-3, replace the original sheets including Fig. 2-3. No new matter has been added.

Attachment: Replacement Sheets

REMARKS/ARGUMENTS

Claims 3-14 are pending. The Office Action rejects claims 1-2 under 35 U.S.C. §101 as non-statutory, under 35 U.S.C. §102 over Herz (U.S. Patent No. 6,088,722), and under 35 U.S.C. §103 over Benantar (U.S. Pub. No. 2002/0144119) in view of Menezes ("Handbook of Applied Cryptography," p. 396-97). By this Amendment, claims 1-2 are canceled and claims 3-14 are new. Support for the amendments can be found at least at paragraphs 0010-15 and throughout the specification, drawings, and claims as originally filed. No new matter has been added.

Information Disclosure Statement

Applicants thank the Examiner for pointing out the clerical error in the IDS submitted September 27, 2005. An IDS and form SB/08 listing the International Search Report and Written Opinion is submitted herewith.

Drawings

The Office Action objects to Figures 2-3 as being handwritten and difficult to read. Replacement drawings are submitted herewith. The replacement drawings present Figures 2-3 in a more legible form; no new matter has been added. Withdrawal of the objections is respectfully requested.

35 U.S.C. §101 Rejections

Claims 1-2 stand rejected under §101 as directed to non-statutory subject matter. These claims have been canceled, rendering these rejections moot. Each of claims 3-14 recite a method or a token, which are statutory subject matter. Withdrawal of the rejections is respectfully requested.

35 U.S.C. §102 Rejections

Claims 1-2 stand rejected as unpatentable over Herz. These claims have been canceled, rendering the rejections moot.

The Office Action characterizes Herz's seed N as a new secret sent to a set top box for each session from which one time passwords K_i are derived. The encrypted seed is then

interpreted as a digital certificate. *See* Office Action, ¶ 8. Regardless of whether the Office's interpretation is correct, which Applicants do not concede, Herz fails to disclose or suggest the features recited in claims 3-14.

Independent claim 3 recites a method for reprovisioning **a token having a first secret** comprising, in relevant part,

> sending a request for a certificate;
> receiving a certificate that contains a **second secret encrypted with a public key of the token**, the second secret **distinct from the first secret**; and
> generating a one time password **based on the second secret**.

Independent claim 9 recites similar features. In contrast, Herz's system uses synchronized pseudo-random number generators to avoid passing a single one time session key back and forth between a set top box and a head end. *See* col. 45:38-51. Herz uses the same pseudo-random number generators at both ends of the communication, and relies on a single seed to coordinate the generators. There is no suggestion that the encrypted seed "certificate" cited by the Office Action includes a second secret distinct from a first secret of the token, or that a second secret is used to generate a one time password. Thus, Herz fails to disclose or suggest at least a certificate containing a second secret distinct from a token's first secret that is encrypted with a public key, and generating a one time password based on the second secret. The dependent claims recite additional features not disclosed by Herz, and also are allowable for at least the same reasons as the independent claims.

35 U.S.C. §103 Rejections

Claims 1-2 stand rejected as unpatentable over Benantar in view of Menezes. These claims have been canceled, rendering the rejections moot.

Benantar describes a single sign-on system that allows a user to access multiple systems using a single certificate. *See, e.g.,* ¶ 0085, 0093, 0098-0104. However, there is no suggestion in Benantar that the certificate can include a second secret distinct from an initial secret at a token, or of using a second secret to generate a one time password as required by independent claims 3

and 9. In fact, Benantar does not disclose a token as required by the claims at all, but rather relies on the user's certificate and stored responses to perform any authentication.

Menezes merely describes conventional one time password schemes, and fails to remedy the defects of Benantar. Specifically, Menezes fails to disclose or suggest a certificate containing a second secret distinct from a token's first secret, or generating a one time password using a second secret. Thus, whether considered alone or in combination, Benantar and Menezes fail to suggest every feature recited in the claims. The dependent claims recite additional features not disclosed by Benantar or Menezes, and also are allowable for at least the same reasons as the independent claims.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 202-481-9900.

Respectfully submitted,

/ASKamlay/
Aaron S Kamlay
Reg. No. 58,813

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 202-481-9900
Fax: 415-576-0300
Attachments
AK:ak
61335343 v1